

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method, comprising:

initializing a virus scanner during a pre-boot phase of a computer system from firmware that is embedded within the computer system in response to a computer system reset, wherein the virus scanner is executing in a virtual machine monitor (VMM) executing on the computer system, the VMM supporting at least one virtual machine (VM) executing on the computer system, wherein the VM executes an operating system that is different from the VMM and the operating systems executed by other VMs and the VMM acts as an input/output (I/O) controller for requests to selected I/O ports;

determining whether to perform a memory scrub based on a platform policy; scrubbing data read from an input/output (I/O[1]) device of the computer system during the pre-boot phase by the virus scanner using a virus signature database before the data is loaded, wherein the virus signature database is stored in a place not exposed to the operating system and is updated during the pre-boot phase; and enacting a platform policy if a virus is detected in the data.

2. (Original) The method of claim 1, further comprising scrubbing contents of a memory device of the computer system during the pre-boot phase by the virus

scanner.

3. (Original) The method of claim 1, further comprising updating the virus signature database with updated virus signatures.

4. (Original) The method of claim 3 wherein the virus signature database is updated during the pre-boot phase.

5. (Original) The method of claim 1 wherein the virus signature database is not exposed to an operating system executing on the computer system.

6. (Original) The method of claim 5 wherein the virus signature database is stored in a firmware-reserved area.

7. (Canceled)

8. (Currently Amended) The method of claim 1 [[7]] wherein scrubbing data read from the I/O device includes:

receiving a request from a requester to read data from the I/O device, the requester in a VM of at least one VM;

loading at least a portion of the requested data into a buffer;

scrubbing the at least a portion of the requested data with the virus scanner;

returning an error signal to the requester if the virus scanner detects a virus in the at least a portion of the requested data; and forwarding the requested data to the requester if the virus scanner does not detect a virus in the at least a portion of the requested data.

9. (Original) The method of claim 1 wherein the virus scanner is operable during the pre-boot phase, an operating system (OS) runtime phase, and an after-life phase of the computer system independent of an operating system of the computer system.

10. (Original) The method of claim 1 wherein the virus scanner scrubs the data without having knowledge of a file system of the data.

11. (Original) The method of claim 1, further comprising enacting the platform policy if the virus scanner detects non-normal behavior within the computer system.

12. (Currently Amended) An article of manufacture comprising:
a machine-accessible medium including a plurality of instructions which when executed perform operations comprising:

initializing a virus scanner during a pre-boot phase of a computer system from firmware that is embedded within the computer system in response to a computer system reset;

determining whether to perform a memory scrub based on a platform policy;

scrubbing data read from an input/output (I/O) device of the computer system during the pre-boot phase by the virus scanner using a virus signature database before the data is loaded, wherein the virus signature database is stored in a place not exposed to the operating system and is updated during the pre-boot phase, wherein scrubbing data read from the I/O device includes:

launching a virtual machine monitor (VMM), the virus scanner to operate from the VMM where the VM executes an operating system that is different from the VMM and the operating systems executed by other VMs and the VMM acts as an input/output (I/O) controller for requests to selected I/O ports; and

launching a virtual machine (VM) to be supported by the VMM; and

generating an error signal if a virus is detected by the virus scanner.

13. (Original) The article of manufacture of claim 12, further comprising receiving updated virus signatures at the computer system to update the virus signature database.

14. (Original) The article of manufacture of claim 12 wherein the virus signature database is stored in a place not exposed to an operating system of the computer system.

15. (Original) The article of manufacture of claim 12 wherein the virus scanner to be operable during the pre-boot phase, an operating system (OS) runtime phase, and an after-life phase of the computer system independent of an operating system

of the computer system.

16. (Original) The article of manufacture of claim 12 wherein the virus scanner to scrub the data without having knowledge of a file system of the data.

17. (Canceled)

18. (Currently Amended) The article of manufacture of claim 12 [[17]] wherein execution of the plurality of instructions further perform operations comprising: receiving a request from a requester in the VM to read data from the I/O device; loading at least a portion of the requested data into a buffer; scrubbing the at least a portion of the requested data with the virus scanner; returning an error signal to the requester if the virus scanner detects a virus in the at least a portion of the requested data; and forwarding the requested data to the requester if the virus scanner does not detect a virus in the at least a portion of the requested data.

19. (Previously Presented) The article of manufacture of claim 12 wherein the plurality of instructions is to operate in compliance with an Extensible Firmware Interface (EFI) specification.

20. (Currently Amended) A computer system, comprising:

a processor;
a memory device operatively coupled to the processor;
a storage device operatively coupled to the processor; and
at least one flash memory device operatively coupled to the processor, the at least one flash memory device including firmware instructions which when executed by the processor perform operations comprising:

initializing a virus scanner during a pre-boot phase of a computer system from the firmware, wherein the virus scanner executes in a virtual machine monitor (VMM) executing on the computer system, the VMM supporting at least one virtual machine (VM) executing on the computer system, wherein the VM executes an operating system that is different from the VMM and the operating systems executed by other VMs and the VMM acts as an input/output (I/O) controller for requests to selected I/O ports;

scrubbing contents of the memory device during the pre-boot phase by the virus scanner using a virus signature database based on a platform profile, wherein the virus signature database is stored in a place not exposed to the operating system and is updated during the pre-boot phase;

scrubbing data read from the storage device to be loaded into memory by the virus scanner using the virus signature database before the data is loaded in the memory device; and

generating an error signal if a virus is detected by the virus scanner.

21. (Original) The computer system of claim 20, further comprising a

network interface operatively coupled to the processor, the virus scanner to scrub data read from the network interface using the virus signature database before the data is loaded in the memory device.

22. (Original) The computer system of claim 20 wherein the virus signature database is stored in a firmware reserved area of the storage device, the firmware reserved area not exposed to an operating system of the computer system.

23. (Original) The system of claim 20 wherein execution of the firmware instructions further perform operations comprising updating the virus signature database with updated virus signatures downloaded from an external virus signature repository communicatively coupled to the computer system.

24. (Original) The computer system of claim 20 wherein the virus scanner is operable during the pre-boot phase, an operating system (OS) runtime phase, and an after-life phase of the computer system independent of an operating system of the computer system.

25. (Original) The computer system of claim 20 wherein the virus scanner to scrub the data without having knowledge of a file system of the storage device.

26. (Previously Presented) The computer system of claim 20 wherein the firmware instructions to operate in compliance with an Extensible Firmware Interface

(EFI) specification.

27-30. (Canceled)